# Temporal Seed — Environmental Entropy as a Distributed Root of Trust

Author: POXUW
Date: March 14, 2026
Document Type: Prior Art / Defensive Publication (Redacted)

## Abstract

This document describes a novel hardware trust architecture where cryptographic seed material is dynamically reconstructed from a rolling history of physically observed environmental events. Moving beyond static secrets stored in memory, this system derives its root of trust from time-dependent physical sensor data and distributed node consensus. Environmental inputs, including ambient light levels, motion-triggered LED pulses, and hardware telemetry, form a continuously evolving entropy log. A dynamically selected historical lookback window is then used to derive a Temporal Seed, which serves as the ephemeral root of trust for authentication and synchronization. The information required to reconstruct this seed is inherently distributed across time, physical space, and environmental context, rendering it thermodynamically irreversible and resistant to single-point capture, replay, or reconstruction attacks. Critical implementation details are intentionally redacted to preserve intellectual property while establishing prior art.

## 1. Introduction: The Challenge of Static Secrets

Conventional hardware security relies heavily on persistent cryptographic secrets, such as private keys or root certificates, stored in secure memory or dedicated hardware modules. While effective against many threats, these static secrets represent a single point of failure. A successful compromise can lead to complete system compromise.

This work proposes a paradigm shift: a trust model where authentication material is not stored but reconstructed from a shared, remembered environmental history. This distributes authentication across temporal history, environmental state, and distributed hardware nodes, removing the concept of a single persistent root secret.

## 2. The Temporal Seed: Entropy from the Environment

The Temporal Seed is an ephemeral cryptographic value derived from a rolling, cryptographically hashed history of environmental observations. Unlike traditional random number generators, entropy sources originate from external physical conditions observed by sensors.

Conceptually:

TemporalSeed = HASH(EnvironmentalLog[DynamicWindowStart : DynamicWindowEnd])

The seed therefore exists only when reconstructed from the correct historical environmental window.

## 3. Distributed Reconstruction and Consensus

Multiple nodes maintain environmental logs and participate in reconstructing the same Temporal Seed. Nodes exchange fragments of sensor history and synchronization signals through distributed communication channels.

Successful reconstruction requires correlated environmental observations and compatible log histories. Capturing a single node does not provide enough information to reconstruct the seed without the broader environmental and temporal context.

## 4. Dual-Channel Communication and Verification

The system uses two communication channels.

Digital Channel: nodes exchange encrypted environmental fragments and synchronization data through wireless or wired networks.

Optical Channel: nodes transmit encoded synchronization signals using modulated light pulses. This confirms physical presence and provides an out-of-band verification mechanism.

## 5. Flicker Synchronization: The Visible Root of Trust

Each node emits a visible light signal derived from the current Temporal Seed.

SignalPattern = f(TemporalSeed, SystemParameters)

Nodes deriving the same seed generate identical visual patterns. A compromised or desynchronized node produces a visibly different pattern, making anomalies observable.

## 6. Ghost Quorum: The Deception Layer

Ghost Quorum introduces decoy nodes that are indistinguishable from operational nodes. These nodes participate in synchronization and emit identical signals but may not participate fully in quorum decisions.

Because attackers cannot distinguish real nodes from decoys, neutralizing any node risks destabilizing the entire system.

## 7. Security Characteristics

The architecture provides several security properties:

• Thermodynamic Irreversibility – the seed depends on past environmental events. • Environmental Entropy – entropy originates from real-world signals. • Temporal Distribution – the seed depends on historical observations. • Spatial Distribution – multiple nodes participate in reconstruction. • Deception Layer – ghost nodes increase attack uncertainty. • Ephemeral Secret – no static secret exists in memory. • Physical Verification – visible flicker synchronization confirms system state.

## 8. Limitations and Future Work

Challenges include environmental divergence between nodes, maintaining synchronization across distributed hardware, and validating entropy robustness under adversarial conditions.

## 9. Origin

The concept originated from observing analog brightness modulation in consumer RGB lighting systems. These variations suggested that subtle environmental signals could provide usable entropy for security systems.

## 10. Conclusion

Temporal Seed proposes a trust model where authentication emerges from shared environmental history rather than stored secrets. By distributing trust across time, environment, and system topology, the architecture aims to improve resilience against physical and digital compromise.